



Takatashi, Ono et al.

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 4月27日

出 願 番 号

Application Number:

平成11年特許願第119442号

出 願 人

Applicant (s):

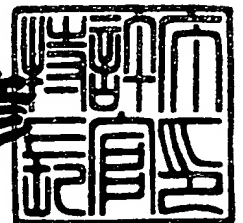
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 3月31日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3022987

【書類名】 特許願

【整理番号】 2022510233

【提出日】 平成11年 4月27日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/06
G09C 1/00

【発明者】

【住所又は居所】 愛知県名古屋市中区栄 2 丁目 6 番 1 号白川ビル別館 5 階
株式会社松下電器情報システム名古屋研究所内

【氏名】 小野 貴敏

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 原田 俊治

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【プルーフの要否】 不要

【書類名】 明細書

【発明の名称】 デジタルコンテンツ利用制御システム

【特許請求の範囲】

【請求項 1】 予め定められた利用条件に従ってデジタルコンテンツの利用を制御し、かつ当該利用条件、当該デジタルコンテンツの不正な使用を防止するためのデジタルコンテンツ利用制御システムであって、

複数の、デジタルコンテンツ、暗号化された利用条件及び暗号化された補助鍵を格納し、かつ情報の読み出し及び書き込みが可能な記録媒体が、デジタルコンテンツを利用する実行器に情報伝達可能に接続され、

前記実行器は、

乱数を格納し、かつ自己の外部からは情報の読み出し及び書き込みが困難な乱数格納手段と、

前記記録媒体から暗号化された補助鍵を獲得して、前記乱数格納手段から取得した乱数で復号する第 1 の復号手段と、

前記記録媒体から暗号化された利用条件を獲得して、前記第 1 の復号手段の復号によって得られた補助鍵で復号する第 2 の復号手段と、

前記記録媒体から対応するデジタルコンテンツを獲得して、前記第 2 の復号手段の復号によって得られた利用条件に従って利用を実行するデジタルコンテンツ利用手段と、

前記第 1 の復号手段の復号によって得られた補助鍵とは異なる新たな補助鍵を生成する補助鍵生成手段と、

前記第 2 の復号手段の復号によって得られた利用条件を、前記デジタルコンテンツ利用手段がデジタルコンテンツを利用した後に、前記補助鍵生成手段によって生成された新たな補助鍵で暗号化して、前記記録媒体に格納する第 1 の暗号化手段と、

デジタルコンテンツの利用に関連して、前記記録媒体から全ての暗号化された補助鍵を獲得して、前記乱数格納手段に格納された乱数で復号する第 3 の復号手段と、

前記第 3 の復号手段の復号に連携して、前記乱数格納手段に格納された乱数を更

新する乱数更新手段と、

前記第 3 の復号手段の復号によって得られた補助鍵から、前記第 1 の復号手段にの復号によって得られた補助鍵を除き、さらに前記補助鍵生成手段によって生成された補助鍵を加えたものを、前記乱数更新手段によって更新された乱数で暗号化して、前記記録媒体に格納する第 2 の暗号化手段とを備える、デジタルコンテンツ利用制御システム。

【請求項 2】 デジタルコンテンツの利用にともなって、前記第 2 の復号手段の復号によって得られた利用条件を更新する利用条件更新手段をさらに備え、前記第 1 の暗号化手段は、前記利用条件更新手段によって更新された利用条件を、前記補助鍵生成手段によって生成された新たな補助鍵で暗号化して、前記記録媒体に格納することを特徴とする、請求項 1 に記載のデジタルコンテンツ利用制御システム。

【請求項 3】 前記第 3 の復号手段は、デジタルコンテンツの利用毎に、前記記録媒体から全ての暗号化された補助鍵を獲得して、前記乱数格納手段に格納された乱数で復号することを特徴とする、請求項 1 または 2 に記載のデジタルコンテンツ利用制御システム。

【請求項 4】 前記補助鍵生成手段は、予め決められた複数回のデジタルコンテンツの利用に一度、前記第 1 の復号手段の復号によって得られた補助鍵とは異なる新たな補助鍵を生成し、

前記第 1 の暗号化手段は、予め決められた複数回のデジタルコンテンツの利用に一度、利用条件を前記補助鍵生成手段によって生成された新たな補助鍵で暗号化して、それ以外の時には、前記第 1 の復号手段の復号によって得られた補助鍵で暗号化して、

前記第 3 の復号手段は、予め決められた複数回のデジタルコンテンツの利用に一度、前記記録媒体から全ての暗号化された補助鍵を獲得して、前記乱数格納手段に格納された乱数で復号することを特徴とする、請求項 1 または 2 に記載のデジタルコンテンツ利用制御システム。

【請求項 5】 前記補助鍵生成手段は、予め決められた可変の回数のデジタルコンテンツの利用に一度、前記第 1 の復号手段の復号によって得られた補助鍵と

は異なる新たな補助鍵を生成し、

前記第 1 の暗号化手段は、予め決められた可変の回数のデジタルコンテンツの利用に一度、利用条件を前記補助鍵生成手段によって生成された新たな補助鍵で暗号化して、それ以外の時には、前記第 1 の復号手段の復号によって得られた補助鍵で暗号化して、

前記第 3 の復号手段は、予め決められた可変の回数のデジタルコンテンツの利用に一度、前記記録媒体から全ての暗号化された補助鍵を獲得して、前記乱数格納手段に格納された乱数で復号することを特徴とする、請求項 1 または 2 に記載のデジタルコンテンツ利用制御システム。

【請求項 6】 前記補助鍵生成手段が補助鍵を生成する間隔に関する情報を、デジタルコンテンツ利用者に秘密にすることを特徴とする、請求項 5 または 6 に記載のデジタルコンテンツ利用制御システム。

【請求項 7】 前記乱数格納手段は、前記実行器に設けられる代わりに、前記記録媒体に設けられることを特徴とする、請求項 1 または 2 に記載のデジタルコンテンツ利用制御システム。

【請求項 8】 前記記録媒体の代わりに、読み出し専用の第 1 の記録媒体と、読み出し及び書き込みが可能な第 2 の記録媒体とが前記実行器に接続され、前記第 1 の記録媒体はデジタルコンテンツを格納し、前記第 2 の記録媒体は暗号化された利用条件を格納し、前記乱数格納手段は、前記実行器に設けられる代わりに、前記第 2 の記録媒体に設けられることを特徴とする、請求項 1 または 2 に記載のデジタルコンテンツ利用制御システム。

【請求項 9】 前記記録媒体に格納されたデジタルコンテンツは、それぞれ暗号化されており、前記デジタルコンテンツ利用手段は、前記記録媒体から、対応する暗号化されたデジタルコンテンツを獲得して、前記第 2 の復号手段の復号によって得られた利用条件に従って復号し、復号して得たデジタルコンテンツの利用をを実行することを特徴とする、請求項 1 または 2 に記載のデジタルコンテンツ利用制御システム。

【請求項 1 0】 前記実行器は個々の実行器に固有の実行器固有鍵を持ち、前記デジタルコンテンツ利用手段は、暗号化されたデジタルコンテンツの復号に、前記実行器固有鍵を用いることを特徴とする、請求項 9 に記載のデジタルコンテンツ利用制御システム。

【請求項 1 1】 前記デジタルコンテンツ利用手段は、暗号化されたデジタルコンテンツと、その復号に用いる鍵を獲得して、その利用を実行することを特徴とする、請求項 9 または 1 0 に記載のデジタルコンテンツ利用制御システム。

【請求項 1 2】 前記乱数更新手段は、前記乱数格納手段に格納された乱数を種に、新たな乱数を生成することを特徴とする、請求項 1 または 2 に記載のデジタルコンテンツ利用制御システム。

【請求項 1 3】 前記乱数更新手段は、前記乱数格納手段に格納された乱数をインクリメントした値を新たな乱数とすることを特徴とする、請求項 1 または 2 に記載のデジタルコンテンツ利用制御システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、デジタルコンテンツ利用制御システムに関し、より特定的には、デジタルコンテンツの不正使用を防止するためのデジタルコンテンツ利用制御システムに関する。

【0 0 0 2】

【従来の技術】

近年、著作権のある情報のデジタル化が進んでいる。特に音楽情報などはデジタル化を行なうことによって音質の劣化を防ぐことができるという利点がある。しかしデジタル化することによって、不正な利用（複製）が簡易に行なわれてしまうという欠点も表面化している。

【0 0 0 3】

このような不正を防ぐために、著作権法などの法整備とともに、デジタルコンテンツの利用制御システムが考案されている。例えば、特開平 9 - 1 8 5 5 0 1 号公報には、デジタルコンテンツの一つであるソフトウェアについて、不正に

コピーされたソフトウェアを利用（実行）できないようにする、ソフトウェア実行制御システムが開示されている。

【0004】

図5は特開平9-185501号公報に係わるソフトウェア実行制御システムの構成を示すブロック図である。図5において、このシステムは、ソフトウェアを格納する記録媒体20と、ソフトウェアを実行する実行器21とを備えている。実行器21は、乱数格納部22と、第1の復号部23と、第2の復号部24と、第3の復号部25と、実行回数検査部26と、実行回数更新部27と、第1の暗号部28と、ソフト実行部29とを含む。

【0005】

図6は、図5のソフトウェア実行制御システムの動作を示すフローチャートである。図6を用いて、図5に示すシステムの動作を説明する。記録媒体20には、ソフトウェアSoft Aに関する情報として、暗号化ソフトE (KA, Soft A) と、暗号化ソフト鍵／実行回数E (RA, (KA, nA)) と、暗号化補助鍵E (R, RA) とが、ソフトウェアSoft Bに関する情報として、暗号化ソフトE (KB, Soft B) と、暗号化ソフト鍵／実行回数E (RB, (KB, nB)) と、暗号化補助鍵E (R, RB) とが、格納されている。ここで、RA及びRBは、それぞれソフトウェアSoft A及びソフトウェアSoft Bに専用の補助鍵であり、E (R, RA) 及びE (R, RB) は、これらをそれぞれ乱数Rで暗号化したものである。

【0006】

乱数格納部22は、読み出し及び書き込みの困難な領域であり、乱数Rを格納している。実行器21は、記録媒体20からソフトウェアSoft Aに関する情報を獲得すると（ステップS301）、第1の復号部23において、乱数Rによって、暗号化補助鍵E (R, RA) を復号し、補助鍵RAを得る（ステップS302）。続いて、実行器21は、第2の復号部24において、この補助鍵RAにより、暗号化ソフト鍵／実行回数E (RA, (KA, nA)) を復号し、ソフト鍵KA及び実行回数nAを得る（ステップS303）。さらに、実行器21は、第3の復号部25において、ソフト鍵KAにより、暗号化ソフトE (KA, So

f t A) を復号し、ソフトウェア S o f t A を得る (ステップ S 3 0 4)。同時に、実行器 21 は、実行回数検査部 26 において、実行回数 $n A$ が 1 以上であるか否かを検査し (ステップ S 3 0 5)、 $n A$ が 1 以上であればソフト実行部 29 に対して実行 OK を通知し、この通知を受けて、ソフト実行部 29 はソフトウェア S o f t A を実行する (ステップ S 3 0 6)。この後、実行回数更新部 27 は、実行回数 $n A$ を 1 減少して $n A'$ ($= n A - 1$) に更新する (ステップ S 3 0 7)。実行回数 $n A'$ は、第 1 の暗号部 28 において、ソフト鍵 $K A$ と共に補助鍵 $R A$ で暗号化され (ステップ S 3 0 8)、この暗号化ソフト鍵/実行回数 $E (R A, (K A, n A'))$ が、記録媒体 20 に再び格納される (ステップ S 3 0 9)。ソフトウェア S o f t B についても、同様にして実行される。

【0007】

このシステムは、ソフトウェアの実行後、所定のタイミングで乱数 R 、及び暗号化補助鍵 $E (R, R A)$ 、 $E (R, R B)$ を更新する。図 7 は、この更新の際の、ソフトウェア実行システムの構成を示すブロック図である。図 7 において、記録媒体 20 は、図 5 におけるものと同様の情報を格納している。実行器 21 は、図 5 におけるものに加えて、第 4 の復号部 30 と、乱数更新部 31 と、第 2 の暗号部 32 とを更に含むが、図には必要な部分だけが表示されている。

【0008】

【発明が解決しようとする課題】

前述した従来例では、ソフト鍵、実行回数とも暗号化されているため、その編集ができず、ソフトウェアの不正使用、すなわちデジタルコンテンツの不正利用を防ぐことができた。しかし $E (R A, (K A, n A))$ をバックアップし、何回かのソフトウェア実行後リストアするという攻撃が可能である。

【0009】

この攻撃を繰り返すことにより、実行回数を暗号化して保持しておくことが無意味となり、永久に利用できてしまうという欠点を持つ。

【0010】

本発明はこの問題を鑑み、たとえ何らかのデータ、例えば前述の従来例では暗号化ソフト鍵/実行回数や、一般的なデジタルコンテンツにおける利用条件など

をバックアップし、デジタルコンテンツの利用後リストアする攻撃に対しても、不正な利用ができないシステムを提供することを目的とする。

【0011】

【課題を解決するための手段】

この課題を解決するために本発明は、デジタルコンテンツの利用に連携して、新たな補助鍵を生成する補助鍵生成手段と、新たに生成された補助鍵を用いて利用条件を暗号化する第1の暗号手段を備えたものである。

【0012】

すなわち本発明は、予め定められた利用条件に従ってデジタルコンテンツの利用を制御し、かつ当該利用条件の不正な使用を防止するためのデジタルコンテンツ利用制御システムであって、複数の、デジタルコンテンツ、暗号化された利用条件及び暗号化された補助鍵を格納し、かつ情報の読み出し及び書き込みが可能な記録媒体が、デジタルコンテンツを実行する実行器に情報伝達可能に接続され、実行器は、乱数を格納し、かつ自己の外部からは情報の読み出し及び書き込みが困難な乱数格納手段と、記録媒体から暗号化された補助鍵を獲得して、乱数格納手段から取得した乱数で復号する第1の復号手段と、記録媒体から暗号化された利用条件を獲得して、第1の復号手段の復号によって得られた補助鍵で復号する第2の復号手段と、記録媒体から対応するデジタルコンテンツを獲得して、第2の復号手段の復号によって得られた利用条件に従って利用を実行するデジタルコンテンツ利用手段と、デジタルコンテンツの利用に連携して、新たな補助鍵を生成する補助鍵生成手段と、第2の復号手段の復号によって得られた利用条件を、デジタルコンテンツ利用に連携して、補助鍵生成手段によって得られた新たな補助鍵で暗号化して、記録媒体に格納する第1の暗号化手段と、デジタルコンテンツの利用に連携して、記録媒体から全ての暗号化された補助鍵を獲得して、乱数格納手段に格納された乱数で復号する第3の復号手段と、第3の復号手段の復号に連携して、乱数格納手段に格納された乱数を更新する乱数更新手段と、第3の復号手段の復号によって得られた補助鍵の中から、第1の復号手段の復号によって得られた補助鍵を除き、補助鍵生成手段によって生成された補助鍵を加えたものを、乱数更新手段によって更新された乱数で暗号化して、記録媒体に格納する

第 2 の暗号化手段とを備えている。

【 0 0 1 3 】

上記のように、本発明は、デジタルコンテンツを利用する実行器と、複数の、デジタルコンテンツ、暗号化された利用条件及び暗号化された補助鍵が格納された記録媒体とで構成される。最初、実行器に備えられた第 1 の復号手段は、記録媒体から、利用すべきデジタルコンテンツに対応する暗号化された補助鍵を獲得し、乱数格納手段に格納された乱数で復号して補助鍵を求める。次に、第 2 の復号手段は、記録媒体から当該デジタルコンテンツに対応する暗号化された利用条件を獲得し、第 1 の復号手段の復号によって求められた補助鍵で復号して、利用条件を得る。デジタルコンテンツ利用手段は、得られた利用条件に従って、当該デジタルコンテンツの利用を実行する。続いて、補助鍵生成手段は、新たな補助鍵を生成し、第 1 の暗号化手段は、補助鍵生成手段によって生成された新たな補助鍵で、得られた利用条件を暗号化して記録媒体に格納する。また、第 3 の復号手段は、デジタルコンテンツの利用実行に関連して、記録媒体から、全ての暗号化された補助鍵を獲得し、乱数格納手段に格納された乱数で復号して補助鍵を求める。第 3 の復号手段の復号に連携して、乱数更新手段は乱数格納手段に格納された乱数を更新する。第 2 の暗号化手段は、第 3 の復号手段の復号によって求められた補助鍵から第 1 の復号手段の復号によって得られた補助鍵を除き、補助鍵生成手段によって生成された補助鍵を加えたものを、更新された乱数で暗号化して記録媒体に格納する。

【 0 0 1 4 】

このように、一つの実行器で複数のデジタルコンテンツを取り扱う場合には、デジタルコンテンツ毎の利用条件をそれぞれに専用の補助鍵で暗号化し、さらに、これらの補助鍵を乱数で暗号化する。そして、デジタルコンテンツの実行に関連して乱数を更新することにより、正規の実行器以外の実行器でデジタルコンテンツ不正に実行されるのを防止することができる。また、取り扱うデジタルコンテンツの数に関わらず、使用する乱数は一つだけでよいため、乱数を格納するための読み出し及び書き込みが困難な記憶領域は、一つの乱数を格納するだけの大きさを備えればよい。

【 0 0 1 5 】

また本発明の別の構成では、前述の発明において、デジタルコンテンツの利用実行にともなって、第 2 の復号手段の復号によって得られた利用条件を更新する利用条件更新手段をさらに備え、第 1 の暗号化手段は、利用条件更新手段によって更新された利用条件を、補助鍵生成手段によって得られた新たな補助鍵で暗号化して、記録媒体に格納することを特徴としている。

【 0 0 1 6 】

このように、上記の発明では、利用条件更新手段が、デジタルコンテンツの利用実行にともなって利用条件を更新し、第 1 の暗号化手段は、利用条件更新手段によって更新された利用条件を、補助鍵生成手段で生成した新たな補助鍵で暗号化する。これにより、コピーされた利用条件の不正な使用、更新された利用条件の記録媒体への書き込み妨害、デジタルコンテンツ利用以前にバックアップされた暗号化利用条件の、不正なリストアを防止することができる。

【 0 0 1 7 】

【発明の実施の形態】

以下、本発明の実施の形態について添付図面を用いて説明する。

【 0 0 1 8 】

図 1 は、本発明の実施形態に係るデジタルコンテンツ利用制御システムの構成を示すブロック図である。図 1 において、本システムは、デジタルコンテンツを格納する記録媒体 1 0 0 と、デジタルコンテンツの利用を実行する実行器 2 0 0 とを備えている。実行器 2 0 0 は、乱数格納部 2 0 1 と、第 1 の復号部 2 0 2 と、第 2 の復号部 2 0 3 と、第 3 の復号部 2 0 4 と、利用条件確認部 2 0 5 と、利用条件更新部 2 0 6 と、補助鍵生成部 2 0 7 と、第 1 の暗号部 2 0 8 と、デジタルコンテンツ利用実行部 2 0 9 と、実行器固有鍵格納部 2 1 0 を含む。

【 0 0 1 9 】

図 2 は、図 1 のデジタルコンテンツ利用制御システムの動作を示すフローチャートである。図 2 を用いて、図 1 に示すシステムの動作を説明する。記録媒体 1 0 0 には、複数のデジタルコンテンツに関する情報が格納されている。ここでは二つの暗号化デジタルコンテンツ E (SK, Music A)、E (SK, Mus

icB)と、それぞれに関する情報として、暗号化利用条件E(KA, InfoA)、E(KB, InfoB)、暗号化補助鍵E(R, KA)、E(R, KB)とが、格納されている。ここでSKは実行器固有鍵、KA及びKBは、それぞれデジタルコンテンツMusicA、MusicB固有の補助鍵、Rは乱数である。またE(K, A)はAをKで暗号化したものを示している。

【0020】

乱数格納部201は、外部から読み出し及び書き込みの困難な領域であり、乱数Rを格納している。また実行器固有鍵格納部210も外部から読みだし及び書き込み困難な領域であり、実行器固有鍵SKを格納している。実行器200は、記録媒体100からデジタルコンテンツMusicAに関する情報を獲得すると(ステップS101)、第1の復号部202において、乱数Rによって、暗号化補助鍵E(R, KA)を復号し、補助鍵KAを得る(ステップS102)。続いて、実行器200は、第2の復号部203において、この補助鍵KAにより、暗号化利用条件E(KA, InfoA)を復号し、利用条件InfoAを得る(ステップS103)。さらに、実行器200は、利用条件確認部205において、デジタルコンテンツMusicAの利用が可能か否かを利用条件InfoAで確認する(ステップS104)。ここでデジタルコンテンツの利用が可能であれば第3の復号部204において、実行器固有鍵SKにより、暗号化デジタルコンテンツE(SK, MusicA)を復号し、デジタルコンテンツMusicAを得て、同時にデジタルコンテンツ利用実行部209でデジタルコンテンツMusicAを利用する(ステップS105)。さらにこのデジタルコンテンツの利用実行と同時に、利用条件更新部206で利用条件InfoAをInfoA'に更新する(ステップS106)。また補助鍵生成部207でKAと異なる補助鍵KA'を生成する(ステップS107)。最後に更新された利用条件InfoA'が第1の暗号部208で補助鍵KA'を使って暗号化され、この暗号化利用条件E(KA', InfoA')が、記録媒体100に再び格納される(ステップS108)。デジタルコンテンツMusicBについても、同様に利用実行される。

【0021】

図3は、本実施形態において、図1、図2に示したデジタルコンテンツMus

i c A の利用後、乱数 R を更新する際の、デジタルコンテンツ利用制御システムの構成を示すブロック図である。図 3 において、記録媒体 1 0 0 は、図 1 におけるものと同様の情報を格納している。実行器 2 0 0 は、図 1 におけるものに加えて、第 4 の復号部 2 1 1 と、乱数更新部 2 1 2 と、第 2 の暗号部 2 1 3 とを更に含むが、図 3 には乱数の更新に必要な部分だけが表示されている。

【 0 0 2 2 】

図 4 は、図 3 に示すシステムの、デジタルコンテンツ M u s i c A の利用後、乱数 R を更新する際の動作を示すフローチャートである。図 4 を用いて、図 3 に示すシステムの動作を説明する。実行器 2 0 0 は、記録媒体 1 0 0 から暗号化補助鍵 E (R , K A) 及び E (R , K B) を獲得する (ステップ S 2 0 1) 。そして第 4 の復号部 2 1 1 において乱数 R で復号して、補助鍵 K A 及び K B を得る (ステップ S 2 0 2) 。この際、実行器 2 0 0 は、乱数更新部 2 1 2 において、乱数格納部 2 0 1 に格納された乱数 R を R ' に更新する (ステップ S 2 0 3) 。また獲得した補助鍵からデジタルコンテンツ M u s i c A の利用条件復号に使われた補助鍵 K A を除き、補助鍵生成部で生成された新たな補助鍵 K A ' を加える (ステップ S 2 0 4) 。続いて、実行器 2 0 0 は、第 2 の暗号部 2 1 3 において、乱数 R ' で補助鍵 K A ' 及び K B をそれぞれ暗号化し (ステップ S 2 0 5) 、これらの暗号化補助鍵 E (R ' , K A ') 及び E (R ' , K B) を記録媒体 2 0 に再び格納する (ステップ S 2 0 6) 。

【 0 0 2 3 】

このように、本実施形態では、利用条件を暗号化するための各デジタルコンテンツ毎の補助鍵と、それらの補助鍵を束ねてそれぞれ暗号化するための乱数 R とを用意して、乱数格納部には乱数 R だけを格納するようにしている。このため、読み出し及び書き込みのできない領域の大きさを最小にすることができて、実現コストも低く抑えることができる。

【 0 0 2 4 】

また利用条件の更新に伴って、その暗号化に使う補助鍵も更新しているため、暗号化利用条件のみ過去にバックアップしたものをリストアして不正利用するという攻撃を防いでいる。また利用条件と補助鍵のペアを、過去にバックアップし

たものをリストアして不正利用しようとしても、補助鍵を束ねて暗号化する乱数も更新していることにより防御している。

【 0 0 2 5 】

【発明の効果】

以上のように本発明によれば、利用条件を不正に複製すること、更新後の利用条件の書き込み妨害に加え、過去の利用条件のバックアップの不正なリストアも防止することができ、その効果は大きい。

【図面の簡単な説明】

【図 1】

本発明の実施形態に係わるデジタルコンテンツ利用制御システムの、デジタルコンテンツを利用する際の構成を示すブロック図

【図 2】

図 1 のデジタルコンテンツ利用制御システムの動作を示すフローチャート

【図 3】

本発明の実施形態に係わるデジタルコンテンツ利用制御システムの、乱数を更新する際の構成を示すブロック図

【図 4】

図 3 のデジタルコンテンツ利用制御システムの動作を示すフローチャート

【図 5】

特開平 9 - 1 8 5 5 0 1 号公報に示されたソフトウェア実行制御システムの、ソフトウェアを実行する際の構成を示すブロック図

【図 6】

図 5 のソフトウェア実行制御システムの動作を示すフローチャート

【図 7】

特開平 9 - 1 8 5 5 0 1 号公報に示されたソフトウェア実行制御システムの、乱数を更新する際の構成を示すブロック図

【符号の説明】

1 0 0, 2 0 記録媒体

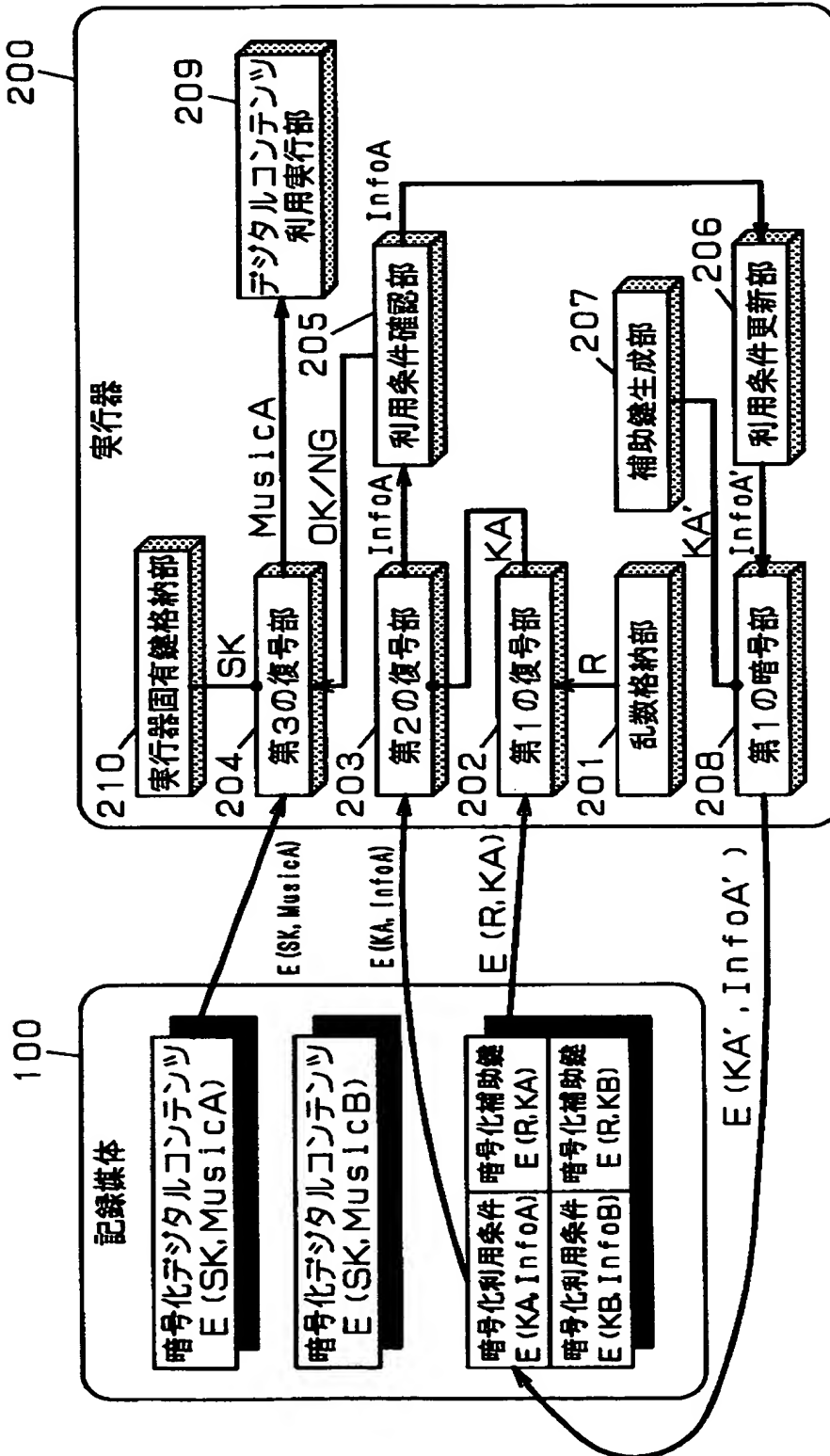
2 0 0, 2 1 実行器

- 2 0 1 乱数格納部
- 2 0 2 第 1 の復号部
- 2 0 3 復号部
- 2 0 4 第 3 の復号部
- 2 0 5 利用条件確認部
- 2 0 6 利用条件更新部
- 2 0 7 補助鍵生成部
- 2 0 8 第 1 の暗号部
- 2 0 9 利用実行部
- 2 1 0 実行器固有鍵格納部
- 2 1 1 第 4 の復号部
- 2 1 2 乱数更新部
- 2 1 3 第 2 の暗号部
- 2 2 乱数格納部
- 2 3 第 1 の復号部
- 2 4 第 2 の復号部
- 2 5 第 3 の復号部
- 2 6 実行回数検査部
- 2 7 実行回数更新部
- 2 8 第 1 の暗号部
- 2 9 ソフト実行部
- 3 0 第 4 の復号部
- 3 1 乱数更新部
- 3 2 第 2 の暗号部

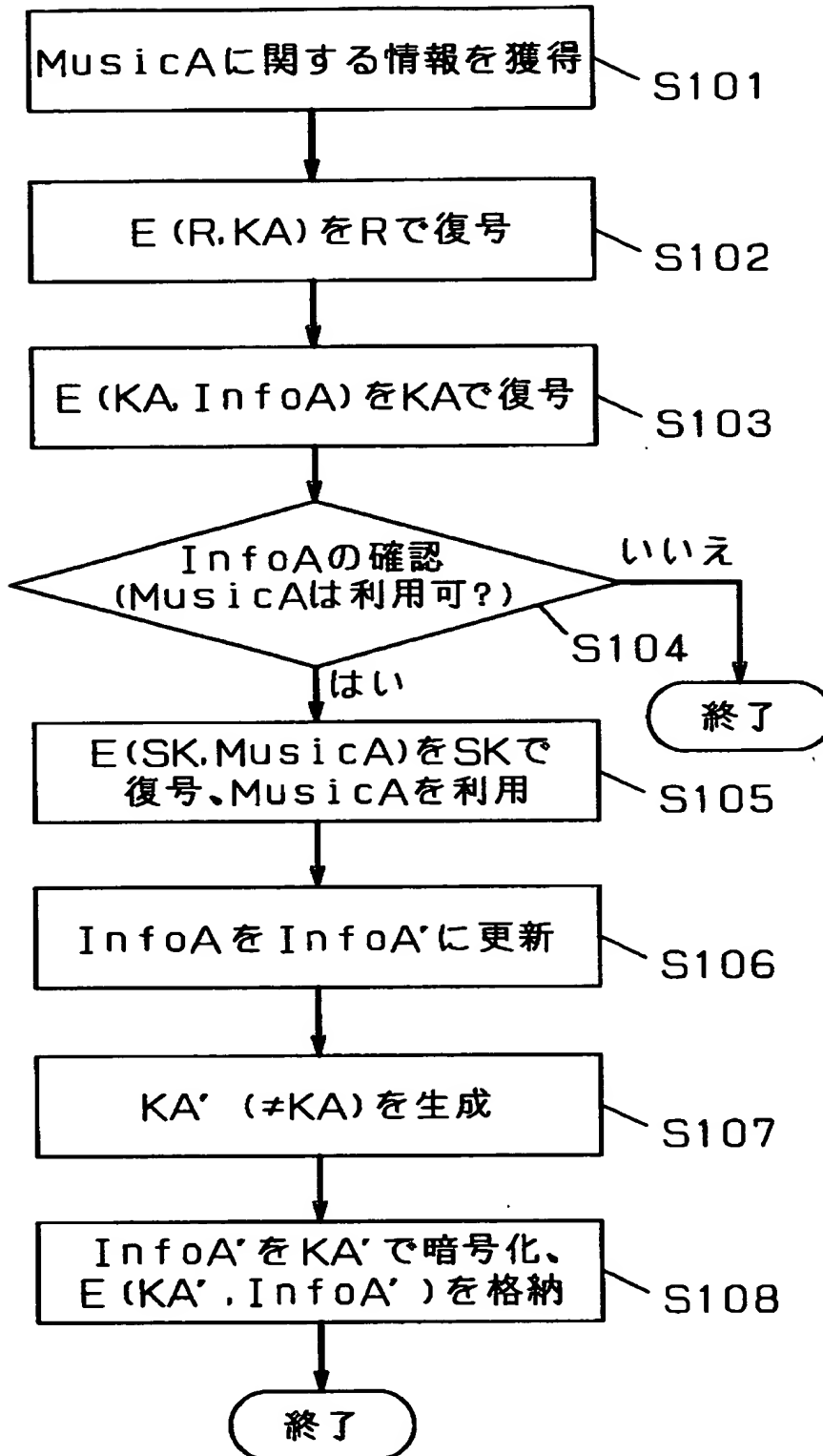
【書類名】

図面

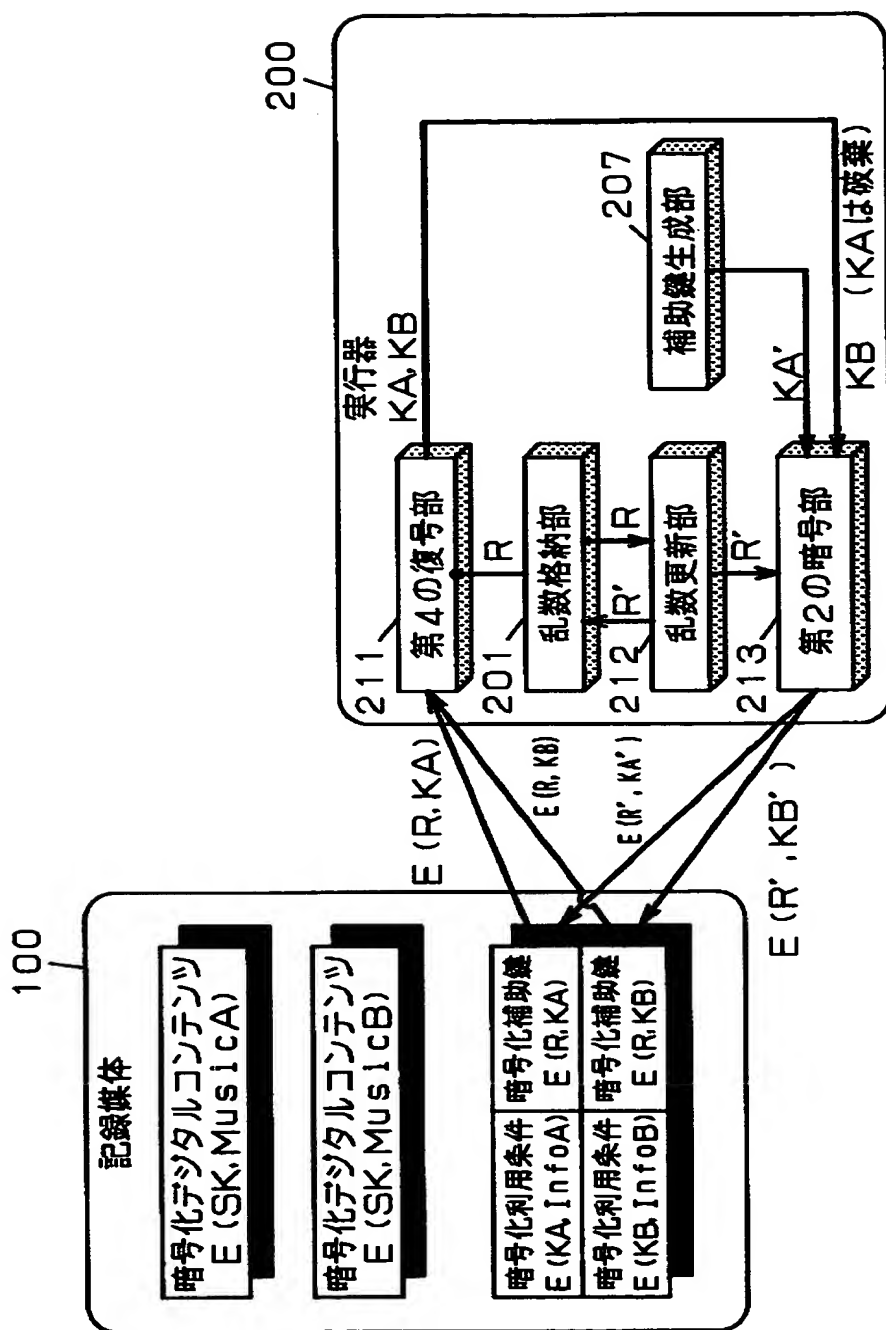
【図 1】



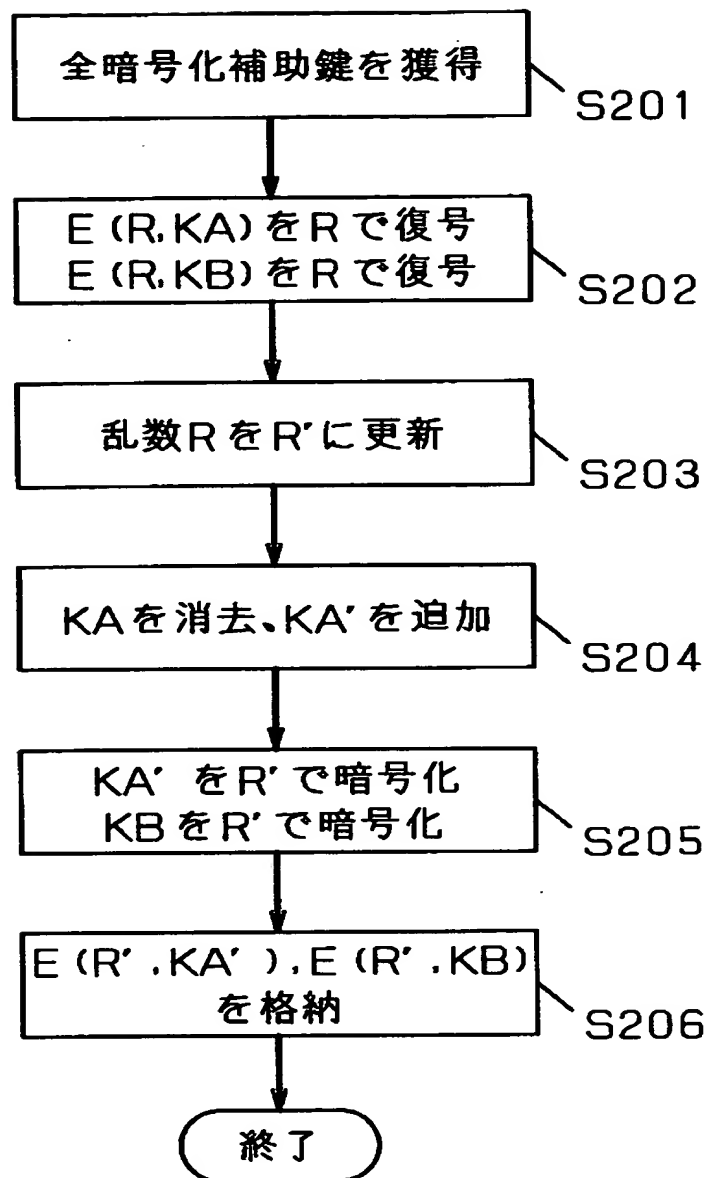
【図 2】



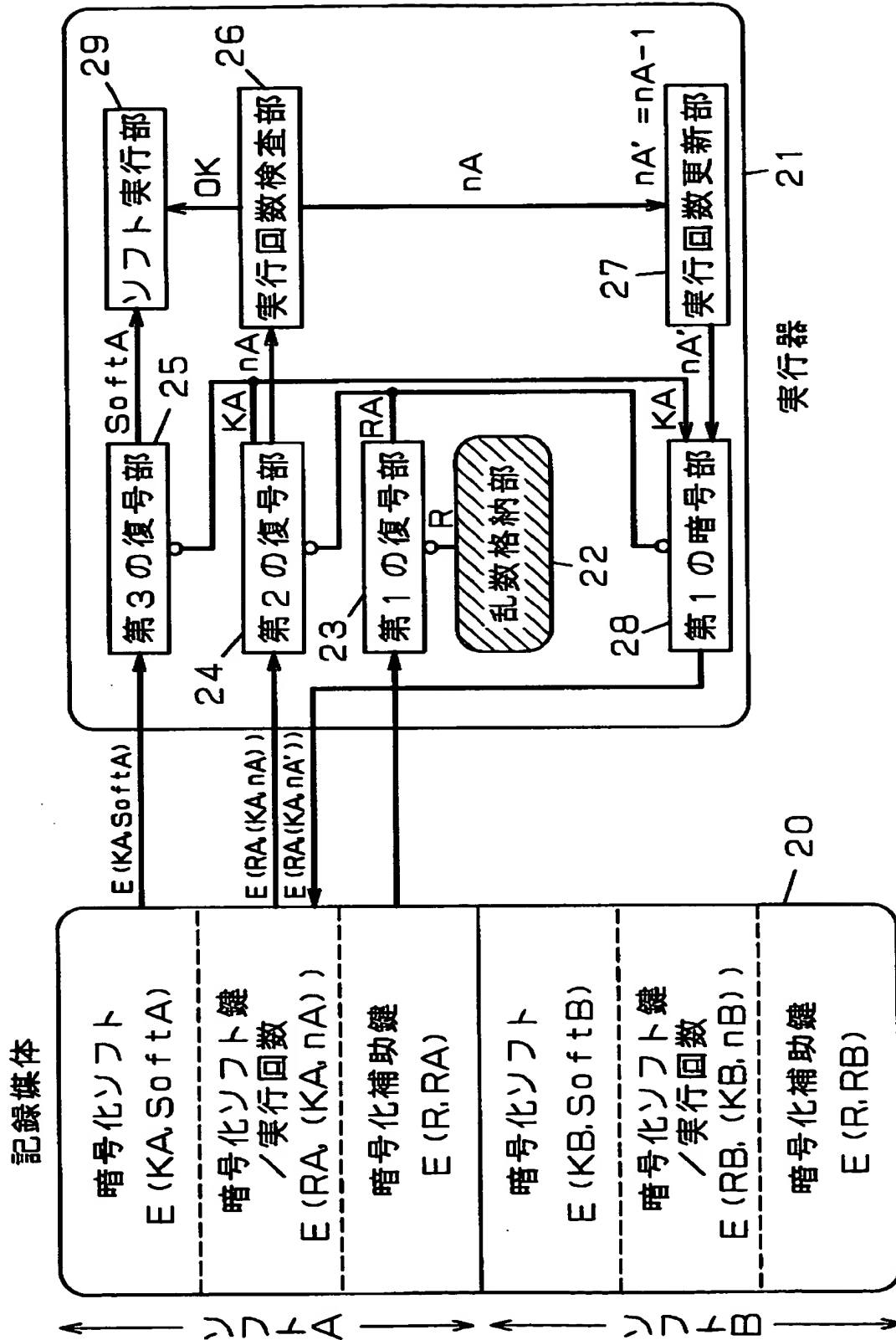
【図 3】



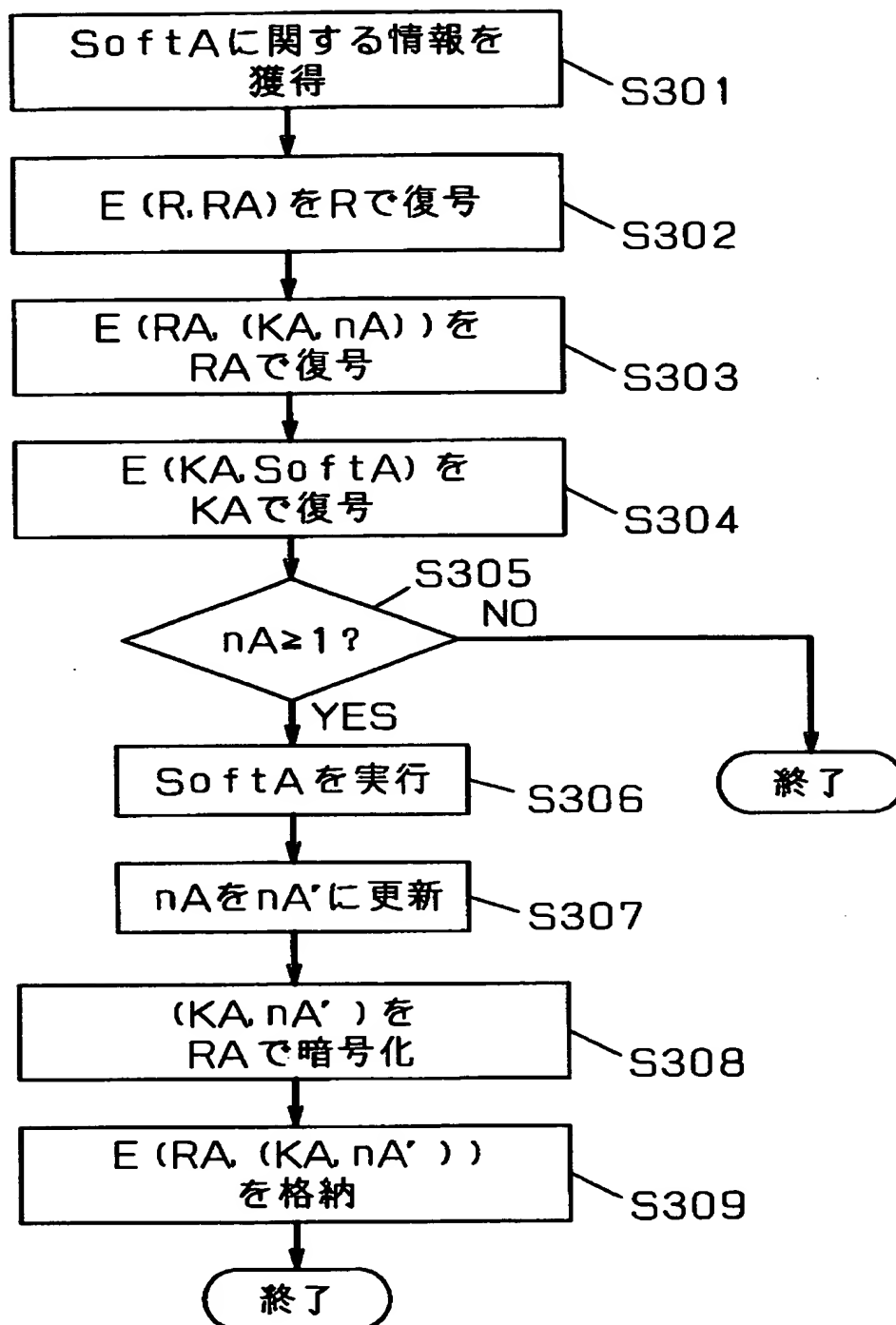
【図4】



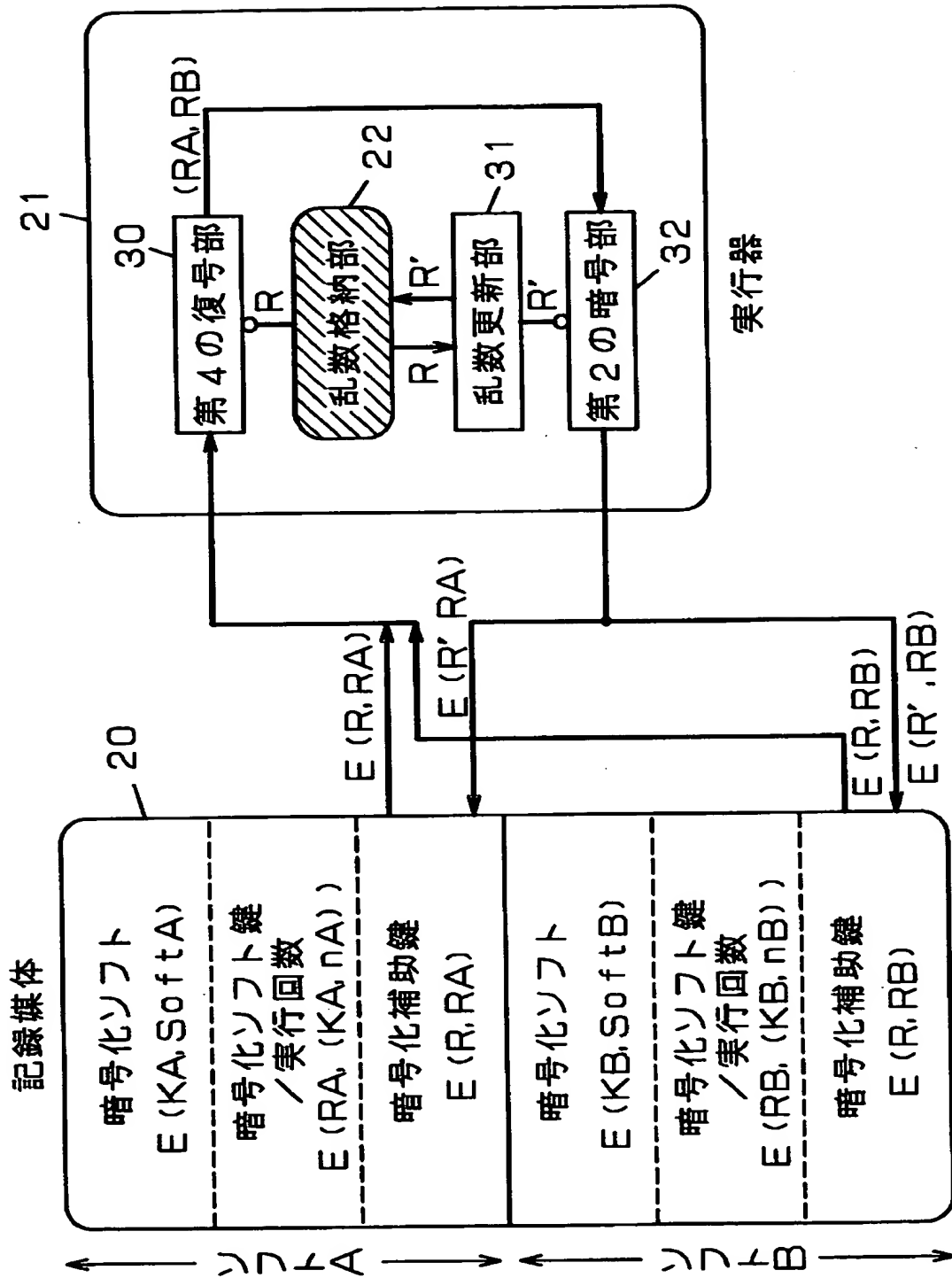
【図 5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 利用条件によりデジタルコンテンツの利用制御を行なうデジタルコンテンツ利用制御システムにおいて、利用条件をバックアップし、デジタルコンテンツの利用後リストアすることによる不正利用を防ぐことを目的とする。

【解決手段】 補助鍵更新手段を設け、利用条件の更新に連携し、利用条件を暗号化する際に用いる補助鍵も更新する。さらに補助鍵は外部から読み書き不能な乱数によって暗号化する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 8 2 1]

1. 変更年月日 1 9 9 0 年 8 月 2 8 日

[変更理由] 新規登録

住 所 大阪府門真市大字門真 1 0 0 6 番地

氏 名 松下電器産業株式会社